现代数学基础丛书

有限群构造

上册

张远达 著

科学出版社

现代数学基础丛书

有 限 群 构 造

上 册

张 远 达 著

科 学 出 版 社

1 9 8 2

现代数学基础丛书

有 限 群 构 造

下 册

张 远 达 著

科 学 出 版 社
1 9 8 2

内 容 简 介

本书主要论述有限群的构造理论，分上、下两册．上册是代数领域中关于有限群的一些基本知识．下册论述有限群的专题部分．

本书可供大专院校数学系高年级学生、研究生及代数研究工作者阅读，也可供其他有关科技工作者参考．

现代数学基础丛书
有限群构造
上 册
张 远 达 著
责任编辑 杜小杨 张鸿林
科 学 出 版 社 出版
北京朝阳门内大街 137 号
中国科学院印刷厂印刷
新华书店北京发行所发行 各地新华书店经售
*
1982 年 11 月第 一 版 开本：850×1168 1/32
1982 年 11 月第一次印刷 印张：13 5/8 插页：1
印数：0001—6,850 字数：357,000
统一书号：13031·2031
本社书号：2778·13—1
定价： 2.55 元

内 容 简 介

本书上册论述了有限群的基本知识，下册着重介绍有限群的一些新成果、发展动向以及有限群的某些较专门的部分，如卡特子群、传输理论、超可解群等.

本书可供大专院校数学系高年级学生、研究生、教师及有关的数学工作者参考.

现代数学基础丛书
有 限 群 构 造
下 册
张 远 达 著
责任编辑 杜小杨 张鸿林
科 学 出 版 社 出 版
北京朝阳门内大街137号
中国科学院印刷厂印刷
新华书店北京发行所发行 各地新华书店经售
*
1982年12月第 一 版 开本：850×1168 1/32
1982年12月第一次印刷 印张：9 3/8
印数：0001—6,940 字数：244,000

统一书号：13031·2105
本社书号：2876·13—1
定价： 1.75 元

《现代数学基础丛书》编委会

序　　言

有限群是代数学中一个古老的分支，它有十分悠久的历史．它是由解代数方程的需要，也就是由伽罗瓦（Galois）理论的需要而产生的，并且首先是由置换群的概念发展起来的．至于群的抽象的讨论大概是从弗罗比尼斯（Frobenius）开始的，也就是后来发现构成群之特殊材料（置换这个概念）并不重要，而只需注意一集合里面所定义的代数运算这个性质的探讨．正是这样一种发展，才使得有限群的一般理论得以建立在公理基础之上而变得严谨且清晰，并有利于这理论的进一步发展．仅在第二次世界大战后期几年它的研究中断了，但不久又恢复了它的活跃力，现在人们对有限群反而更为重视，考其原因是群论几乎在各个科技领域里都有它的应用．在爱丁堡举行的国际数学会上由维兰德（H. Wielandt）作的题为《有限群构造之发展》的报告（文献［1］），以及由居里亨（C. A. Чунихин）在全苏第三届代数会上作的题为《近年来有限群发展的若干方向》的报告（文献［2］），并由最近出版的虎拍（B. Huppert）的巨著（文献［3］），都足以说明近年来有限群研究的盛行．

有限群之研究大体可分为群表现与群构造两个方面．本书只叙述了有限群表现的基本知识，目的是用它证明 p^aq^b 阶群的可解性　本书主要是叙述有限群的构造理论．有限群构造的内容也非常丰富，不可能在一本书内包括无遗．例如，近年来国际上对于有限单群的研究有很大的发展，而本书对这个问题却未触及．本书仅环绕有限可解群能分解为西洛（Sylow）基底，以之为中心来阐述近来的发展趋势，而对超可解群给以较详尽的论述．

全书分上、下两册．上册共五章．第一章是基础理论；第二章以有限可解群能分解为素数幂阶群之积以及这样分解之唯一性

来说明素数幂阶群（在本书中称为 p-群）之重要性；第三章论述群表现的基本知识，解决 p^aq^b 阶群之可解性；第四章讲扩展理论，其重要性有二：一为借它可由二个群怎样去作另一新的群，二为因有限群存在合成群列，故知研究有限群的根本问题是决定有限单群与探索扩展理论；第五章讨论 p-群的基本性质．总而言之，上册为基本概念，是代数领域中关于有限群的一些基本知识，当然间或有些不是为专攻有限群工作的同志所需的内容；凡是这样的地方均打有星号 *，或用小号字排印，像这样一些地方初学者也可略去．

下册论述有限群的专题部分，诸如弗拉梯尼（Frattini）子群，费丁（Fitting）子群，卡特（Carter）子群，恩格尔（Engel）子群，群之 Π-性质及分解，半单群，超可解群，传输理论等等．概括之，本书是以霍尔（P. Hall），柏额（R. Baer），虎拍，维兰德，居里亨等人的主要工作为基础而阐述的，其间并非无作者的创意在．由于有限群范围过大，而本人学识肤浅，错误难免且取材可能不当，望同好者批评指正．

张 远 达

武汉大学，1980 年 8 月

下 册 前 言

本书上册只叙述了有限群的基本知识，间或也提到了某些专题. 在下册里将专门探讨有限群近年来的发展以及它的较艰涩的部分，例如卡特（Carter）子群、恩格尔（Engel）群、正则p-群、传输理论、群之分解及Π-性质、半单群、超可解群等. 有些部分如群之分解及Π-性质，本书都只扼要地讲了其中有代表性的一个或两个问题，不可能一一列举，且没有这个必要. 又如恩格尔群，本书也只讲了一些基本知识，至于深入的部分及一些具有代表性的工作，都只列举了有关的文献，以便使从事这方面工作的同志有处查询. 我们仅将超可解群比较完整地叙述了一番. 总之，本书的目的是使读者明了有限群的基本理论和方法(上册)，同时也介绍一些新成果及动向(下册).

有限群的核心问题是决定所有的单群，这是迄今尚未完全解决的问题. 虽然，最近二十多年在这方面已取得了一些很深刻的结果，使得上述问题的解决现在看来不再是不可能的了，可是这些结果的证明往往篇幅过长且又极为复杂，以至无法在本书内给以详细表述. 本书仅建立一些基本结论与概念，熟悉它们是从事这一学科工作的前提，我们只是抛砖引玉，希望同好者提出批评指正.

张远达

武汉大学 1980 年 9 月

目　　录

目　　录

第一章　基础理论

群的概念在数学各分支与其他科技领域里有广泛的应用．为使读者阅读方便，本书是从群定义及它的一些基本性质开始来叙述的．

§1. 群的概念

定义　由一些同类的元素(例如数或矩阵等等)组成的一个非空集合G满足下列四条件时，就把G叫做群：

1°. 在集合G内定义了一种代数运算——即对G之任二元a，b(a，b可为一同元，也可不同）总可在G中找得一元与它们相应．习惯上叫这样所找得的元素为a与b的积，记作ab（或$a\cdot b$)，并叫a与b都是积ab之因子．注意，积与它的因子之先后顺序有关，即ab与ba一般不见得相等．

2°. 结合律成立——即对G之任三个元a，b，c，常有关系式$(ab)c=a(bc)$．

3°. G中至少有这样一元e，使$ex=x$恒成立(任$x\in G$)．——叫这e为G之一个左单位元．

4°. 对每个$x\in G$，G中至少有这样一元x^{-1}具有性质$x^{-1}x=e$，但这e为3°中所说的某确定的e．于是x^{-1}不仅与x有关且还与e之选择有关叫x^{-1}为x的一个左逆元(对e而言)．

说确切些，又把G关于1°之结合方法叫做群．1°中说的结合方法叫**乘法**．注意，**乘法**与**积**只是两个术语，说明群元素结合的意义与结合的结果．如将群元素结合方法写为加法“+”，则a，b结合的结果为$a+b$，叫做**和**，而结合律应改为$(a+b)+c=a+(b+c)$．

群之左单位元及每元 x 之左逆元 x^{-1} 究竟有怎样的特性呢?

首先，设 e 为群 G 之一左单位元. 对这 e 言，若 $x\in G$ (符号 $x\in G$ 表 x 为 G 之元)，则由 4° 知有 $x^{-1}\in G$，因之又有 $(x^{-1})^{-1}\in G$，使 $x^{-1}x=e$，$(x^{-1})^{-1}\cdot x^{-1}=e$，于是 $(x^{-1}x)x^{-1}=ex^{-1}=x^{-1}$，故再据 2° 得 $x^{-1}(xx^{-1})=x^{-1}$，据 3° 得 $(x^{-1})^{-1}[x^{-1}(xx^{-1})]=(x^{-1})^{-1}x^{-1}=e$，复由 2° 与 3° 得 $e=[(x^{-1})^{-1}x^{-1}](xx^{-1})=e(xx^{-1})=xx^{-1}$. 证得了 $x^{-1}x=xx^{-1}=e$，即对 e 言知 G 中每元 x 之每个左逆元 x^{-1} 必同时为 x 的右逆元. 正因为如此，故无必要把逆元加以左、右之分，干脆叫 x^{-1} 为 x 之逆元，也说明了原先直接用符号 x^{-1} 的用意. 须注意的是，x 的每个逆元 x^{-1} (关于 e 言) 还是唯一的，因若 x_1 是 x 之任一个逆元，则从 $xx_1=e=xx^{-1}$，得 $x^{-1}(xx_1)=x^{-1}(xx^{-1}),(x^{-1}x)x_1=(x^{-1}x)x^{-1},ex_1=ex^{-1},x_1=x^{-1}$，即证明了逆元的唯一性，且同时证明了 x^{-1} 之逆元为 x，即 $(x^{-1})^{-1}=x$.

其次，由 $xe=x(x^{-1}x)=(xx^{-1})x=ex=x$，又知每左单位元 e 同时必为右单位元，因而也无必要将单位元加以左、右之分；干脆叫 e 为 G 之单位元. 群 G 之单位元也是唯一的：因若 e' 是一单位元，则由 e 与 e' 都可为左、右单位元，就不得不有 $ee'=e'$ 与 $ee'=e$，故 $e'=e$.

总之，群 G 的单位元 e 只有一个，每元 x 的逆元 x^{-1} 也只有一个.

如将群定义中的条件 3° 与 4° 分别改为：

3_1°. G 中至少有一右单位元 e 使 $xe=x$ 对任 $x\in G$ 常成立；

4_1°. 对每 $x\in G$，G 中至少有一元 x^{-1} 使 $xx^{-1}=e$ (叫 x^{-1} 为 x 的一个右逆元)，但 e 是 3_1° 中说的某个 e；那末同样可证由 3_1° 与 4_1° 能得 3° 与 4°. 换言之，1°，2°，3°，4° 和 1°，2°，3_1°，4_1° 是群定义的等价条件，即把群定义中的“左”字都改为“右”字，是无影响的.

于是我们自然会问：若将 3° 与 4° 中某个“左”字不变，另一个“左”字改为“右”字，会发生什么现象呢? 如

$$e_1=\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix},\quad e_2=\begin{pmatrix}1 & -1\\ 0 & 0\end{pmatrix},$$

$$a=\begin{pmatrix}-1 & 1\\ 0 & 0\end{pmatrix},\quad b=\begin{pmatrix}-1 & -1\\ 0 & 0\end{pmatrix},$$

这四个 2 级矩阵组成的集合 G 中若定义二元之结合方法为矩阵之通常的乘法，那末 G 中任二元结合之结果如下表所示.

	e_1	e_2	a	b
e_1	e_1	e_2	a	b
e_2	e_1	e_2	a	b
a	b	a	e_2	e_1
b	b	a	e_2	e_1

即先画两条互相垂直的线(一是水平的、另一是竖直的)；再将 G 之元 e_1, e_2, a, b 写在水平线上方，同时又写在竖直线之左方；G 中二元结合时，约定第一个因子取在竖直线的左方，第二个因子取在水平线的上方，并将结合结果写在第一个因子的向右及第二个因子的向下的交叉点处.

从上表看出集合 G 满足群定义条件 1°；因矩阵乘法确满足结合律，故集合 G 满足群定义条件 2°；又从上表已看出 e_1 与 e_2 皆可充当 G 之左单位元，即 3° 成立；但关于 e_1 言确知 e_1, e_2, a, b 的右逆元各为 e_1, e_1, b, b，而对 e_2 言又知它们的右逆元各为 e_2, e_2, a, a 故 G 满足 4_1°. 这说明了 G 满足 1°, 2°, 3°, 4_1°；但 G 不是群，因群之左单位元必为右单位元，而 e_1 与 e_2 都不是右单位元.

由此例可知判断一集合为群时除检验 1°, 2° 外，还需检验 3° 与 4° 同时成立 (或检验 3_1° 与 4_1° 同时成立)，光检验了 3° 与 4_1° (或 3_1° 与 4°) 是不行的.

当结合方法 1° 写为加法"+"时，常用符号"0"表示单位元，用 $-a$ 表示 a 之逆元，习惯上叫这样的群为**加群**. 结合法写为乘法的群叫**乘群**，乘群的单位元有时用 1 表示.

群条件 1° 只是说群之任二元 x，y 结合的结果 xy 与 yx 都是群之元，并不要求 $xy = yx$. 特当群中任二元 x，y 常有关系式 $xy = yx$ 时，叫群为**交换群**. 结合方法写为加法的群习惯上总是表示交换群(即 $x + y = y + x$ 常成立).

只含有限多个元的群 G 叫**有限群**（或叫 G 的**阶**为有限的），否则就说 G 为**无限群**(或叫 G 的**阶**为无限). 通常用符号 $o(G)$ 表示群 G 的阶，例如 $o(G) = \infty$ 表 G 为无限群，而 $o(G) = n$ 表 G 为有限群，其阶等于 n，或叫 G 为 n 阶群.

有限、无限、交换、非交换群的例很多. 如一切正实数之集合是无限交换(乘)群；一切 n 级满秩矩阵(矩阵的要素即组成分子为某域内的元)的集合是无限非交换(乘)群；1 之 n 个 n 次单位根（即方程 $x^n - 1 = 0$ 之根)之集合是 n 阶(有限阶)交换群；由

$$e = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad d = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

这六个 3 级初等矩阵(满秩的)所成之集合关于矩阵之乘法言确成群，而为六阶(有限阶)非交换群，这可以像前面由四个 2 级矩阵列表那样去检验，这时的表如下(叫做群表)：

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

与群定义中条件 1°，2°，3°，4° 等价的除了 1°，2°，3_1°，4_1° 外，

还有另一组等价条件，即 1°, 2° 与

5°. 对于集合 G 中任二元 a 与 b，方程 $ax=b$ 与 $ya=b$ 在 G 内都有解.

由 1°, 2°, 3°, 4° 易知 5°：因为 $x=a^{-1}b$ 与 $y=ba^{-1}$ 显然分别为 $ax=b$ 与 $ya=b$ 的解. 故需检验的是 1°, 2°, 5° $\Longrightarrow$ 3°, 4° [甲 $\Longrightarrow$ 乙表示由甲可推得乙]. 这也易于了解：因对某 $a\in G$，由 5° 可知 $ya=a$ 在 G 内可解，令 e 为其一解 $(ea=a)$，于是对 $b\in G$ 而根据 5° 取 $ax=b$ 之一解 c 后 $(ac=b)$，就有 $eb=e(ac)=(ea)c=ac=b$，证明了 e 为 G 之一左单位元，即 3° 成立；又 $ya=e$ 之解的存在性（条件 5°）即证明了条件 4°.

下一性质很重要，经常引用，即

6°. 在群 G 内方程 $ax=b$ 与 $ya=b$ 的解皆是唯一的.

因从 $ax=b$ 得 $a^{-1}(ax)=a^{-1}b$，而 $a^{-1}(ax)=(a^{-1}a)x=ex=x$，故 $x=a^{-1}b$，即 $ax=b$ 之解只能是 $x=a^{-1}b$. 同样可证 $ya=b$ 之解的唯一性.

注意 这性质 6° 的含义是消去律，即

$$\begin{cases} ax=ax_1\Rightarrow x=x_1, \\ ya=y_1a\Rightarrow y=y_1. \end{cases}$$

特当 G 为由有限多个元而成之集时，易证 G 成群的充要条件是1°, 2°与6°.（即这时不要求5°之可解性，而只要求解之唯一性.）

因若 G 成群，则 1°, 2°, 6° 成立自明. 故需检验的是1°, 2°, 6° $\Longrightarrow$ 5°：因集合 G 只含有限多个元，如以 $a_1, a_2, \cdots, a_n$ 表示。故取定了 G 之某元 a 并作 n 个乘积 $aa_1, aa_2, \cdots, aa_n$ 后，则据 1，知 $aa_i\in G(i=1,2,\cdots,n)$，再据 6° 又知当 $i\neq j$ 时确有 $aa_i\neq aa_j$，于是 $aa_i(i=1,2,\cdots,n)$ 不得不为 G 之全部元素，故不论 b 为 G 之任何元，恒有一 a_i 使 $aa_i=b$（i 随 b 而变化），即 $ax=b$ 在 G 内可解. 同理也知 $ya=b$ 在 G 内可解. 因而 5° 获证.

总之，判定集合 G 成群，有下列三组条件（等价的）：

（一）1°, 2°, 3°, 4°；

（二）1°, 2°, 3_1°, 4_1°；